IN THE CLAIMS:

Please amend the claims as follows:

1. (Currently Amended) A method for the generation of forgery-proof documents or data records, whereby key information is generated and whereby encrypted checking information is formed from the key information and from a transaction indicator,

~~characterized in that~~

~~this objective is achieved in that the generation of the~~ comprising the steps of

generating random key information and ~~the formation of the~~ forming encrypted checking information from the key information and from ~~the~~ a transaction indicator ~~are carried out~~ in a cryptographically reliable contact station,

encrypting the key information in ~~that~~ the cryptographically reliable contact station ~~encrypts the key information, and in that,~~

transmitting the encrypted checking information and the encrypted key information ~~are transmitted~~ by the cryptographically reliable contact station to an intermediate station, ~~in that~~

the intermediate station temporarily ~~stores~~ storing the encrypted key information and the encrypted checking information and ~~transmits it~~ subsequently transmitting this to a cryptographic module of a document producer ~~later on,~~ at a different point in time from the transfer between the cryptographically reliable contact station and the intermediate station.

2. (Currently Amended) The method according to Claim 1,

~~characterized in that~~ comprising generating

the key information ~~is generated~~ in such a way that the key information is formed randomly.

3. (Currently Amended) The method according to ~~one or more of the preceding claims,~~

~~characterized in that~~ Claim 1, comprising configuring at least one of

the encrypted key information ~~and/or~~ and the encrypted checking information ~~is configured~~ in such a way that it cannot be decrypted in the intermediate station.

4. (Currently Amended) The method according to ~~one or more of the preceding claims,~~

~~characterized in that~~ Claim 1, comprising

the cryptographic module ~~preferably decrypts~~ decrypting the key information with a key contained in the cryptographic module.

5. (Currently Amended) The method according to ~~one or more of the preceding claims,~~

~~characterized in that~~ Claim 1, comprising

the document producer ~~enters~~ entering his own data into the cryptographic module.

6. (Currently Amended) The method according to ~~one or more of the preceding claims,~~

~~characterized in that~~ Claim 1, comprising irreversibly linking

the data entered by the document producer ~~is irreversibly linked~~ to the key information by means of the cryptographic module.

7. (Currently Amended) The method according to Claim 6,

~~characterized in that~~ comprising irreversibly linking

the data entered by the document producer and the decrypted key information ~~are irreversibly linked in that~~ by using the key information ~~is used~~ to form a check value for the document.

8. (Currently Amended) The method according to ~~one or both of Claims~~ Claim 6 ~~or 7,~~

~~characterized in that~~, comprising forming at least one of a document and a data record from

the result of the irreversible linking of the data entered by the document producer with the decrypted key information ~~forms a document and/or a data record that is transmitted~~ and transmitting the document or data record to a checking station.

9. (Currently Amended) The method according to Claim 8,

~~characterized in that~~ wherein

the document or data record transmitted to the checking station contains the document producer's own data, at least partially in plain text.

10. (Currently Amended) The method according to ~~one or both of Claims~~ Claim 8 ~~or 9,~~

~~characterized in that~~, comprising entering

the encrypted checking information ~~is entered~~ into the document or data record that is transmitted to the checking station.

11. (Currently Amended) The method according to ~~one or more of the preceding claims,~~

~~characterized in that~~ Claim 1, comprising encrypting

information remaining in the cryptographic module ~~is encrypted~~ in such a way that it can be decrypted in the cryptographic module.

12. (Currently Amended) The method according to ~~one or more of the preceding claims,~~

~~characterized in that~~ Claim 1, supplying

~~the supply of~~ the cryptographic module with the information, also in case of a supply via communication partners that are not reliable in the cryptographic sense, ~~is carried out~~ by a cryptographically reliable station whose information can be relied on by the checking station.

13. (Currently Amended) The method according to Claim 12,

~~characterized in that,~~

in order for a reliable station to provide reliable information for the cryptographic module, using cryptographic encryptions ~~are used~~ that the checking station can reverse.

14. (Currently Amended) The method according to ~~one or more of the preceding claims,~~

~~characterized in that~~ Claim 1, comprising supplying

~~the supply of~~ the cryptographic module via communication partners that are cryptographically non-reliable ~~is carried out~~ in such a way that the information is forwarded to the cryptographic module at a different point in time.

15. (Currently Amended) The method according to ~~one or more of Claims~~ Claim 1 ~~to 14,~~

~~characterized in that~~, comprising supplying

~~the supply of~~ the cryptographic module via communication partners that are cryptographically not reliable ~~is carried out~~ in such a way that an exchange of information within a dialog is not necessary.

16. (Currently Amended) The method according to ~~one or more of Claims~~ Claim 1 ~~to 14,~~

~~characterized in that~~, comprising cryptographically linking

the two types of data ~~are cryptographically linked~~ to each other, ~~but~~ such that said linking cannot be discovered by means of crypto-analysis.

17. (Currently Amended) The method according to Claim 19,

~~characterized in that~~ wherein

the cryptographic linking of the two types of data is such that non-linear fractions are added that are known only to the reliable contact station and to the checking station.

18. (Currently Amended) The method according to ~~one or more of the preceding claims,~~

~~characterized in that~~ Claim 1, wherein

the generated forgery-proof documents or data records contain monetary value information.

19. (Currently Amended) The method according to Claim 18,

~~characterized in that~~ comprising cryptographically connecting

the monetary value information ~~is cryptographically connected~~ to the document or data record in such a way that a check value can be formed by comparing the monetary value information to the document or data record.

20. (Currently Amended) The method according to ~~one or both of Claims~~ Claim 18 ~~or 19,~~

~~characterized in that~~, wherein

the monetary value information contains proof of the payment of postage amounts.

21. (Currently Amended) The method according to Claim 20,

~~characterized in that~~ comprising linking

the monetary value information that proves the payment of postage amounts ~~is linked~~ to identification data of the document producer.

22. (Currently Amended) The method according to ~~one or both of Claims~~ Claim 20 ~~or 21,~~

~~characterized in that~~, comprising linking

the monetary value information ~~is linked~~ to address data.

23. (Currently Amended) A value transfer center with an interface for loading monetary values,

~~characterized in that~~

~~the value transfer center contains~~ comprising an interface to receive encrypted information of a cryptographically reliable contact station and to temporarily store the received encrypted information as well as means for receiving value transfer requests by at least one cryptographic module and of forwarding the received encrypted information to the cryptographic module at a different point in time.

24. (Currently Amended) The value transfer center according to Claim 23,

~~characterized in that~~ wherein

the information is encrypted in such a way that it cannot be decrypted in the value transfer center.